REMARKS

In response to the above-identified Office Action, Applicants amend the application and seek reconsideration thereof. In this response, Applicants amend Claims 1, 11, and 18, and cancel Claims 10, 17, and 22. Applicants do not add any new claims. Accordingly, Claims 1-9, 11-16, 18-21, and 23-26 are pending.

I. Claims Rejected Under 35 U.S.C. § 103(a)

A. Claims 1- 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,748,539 issued to Lotspiech ("Lotspiech") in view of U.S. Pre-Grant Patent Publication No. 2001/0032088 applied for by Utsumi et al. ("Utsumi") and further in view of U.S. Pre-Grant Patent Publication No. 2001/0020254 applied for by Blumenau et al ("Blumenau"). Applicants respectfully traverse the rejection.

To establish a *prima facie* case of obviousness, the Examiner must show the cited references, combined, teach or suggest each of the elements of a claim. Amended Claim 1 recites:

"a number generator housed in a host device to generate a nonce; and

an encryption subsystem housed in a storage device to encrypt data .... using an encryption bus key prior to transmitting the encrypted data via a data bus to the host device in which the encrypted data is to be decrypted, and said encryption bus key is derived based on.... the nonce received over the data bus from the number generator." (Emphasis added). Applicants submit that none of the cited references teach or suggest these elements.

Lotspiech discloses a system in which encryption is performed by a kiosk computer (a processor) and decryption is performed by a player-recorder (another processor) (col. 3, lines 19-20). The media ID, which is characterized as the nonce, is updated or generated by the kiosk. The kiosk does not decrypt the contents of the flash memory. Rather, any player-recorder provided with device keys is capable of decrypting the content.

By contrast, in the claimed device, data is encrypted based on a nonce generated (by a random number generator) in a host device and is decrypted by the same host device. This feature is not taught or suggested by any of the cited references. As mentioned above, any player -recorder of Lotspiech having the device keys is able to decrypt the data. The kiosk that generating the media ID is not even equipped with decryption capabilities. Thus, Lotspiech does not teach or suggest a host device that generates a nonce and decrypts the data that is encrypted based on the nonce, as in amended Claim 1.

Moreover, the player-recorder of Lotspiech would not be able to distinguish the unauthorized copy from a legitimate one, because both copies would have the same information (including the same media ID) required for decryption and replay. Lotspiech's system is capable of protecting against replay attacks only after the flash memory is checked back into the kiosk where the media ID is altered (col. 5, lines 28-35). The claimed device ensures data security by requiring that the same host device be in control of both the nonce generation and data decryption. Another host having the device keys would not be able to replay the data contents, because it would not know the nonce based on which the data contents are encrypted. Even if an attacker makes a copy of the encrypted content, a host would not be able to decrypt the data without knowing the nonce.

The Examiner relies on Utsumi for teaching an encryption subsystem housed in a storage device. However, Utsumi does not cure the defect of Lotspiech for failing to disclose any host device that generates a nonce and decrypts the data that is encrypted based on the nonce. Further, in Utsumi, both encryption and decryption operations are performed by a drive. The concept of ensuring data security between a host and a storage device is totally lacking.

Even assuming for the pure sake of argument that the kiosk of Lotspiech is replaced by a drive of Utsumi, there is still no teaching or suggestion that the same host device generates a nonce and decrypts the data that is encrypted based on the nonce. The concept of generating a nonce is totally lacking in Utsumi. Thus, the proposed combination would not produce the device as claimed.

The Examiner relies on Blumenau for teaching a data bus connecting to a destination in which the encrypted data is to be decrypted. However, Blumenau also fails to disclose a host device that generates a nonce and decrypts the data that is encrypted based on the nonce. In Blumenau, the random number is generated by a storage device rather than a host device. Further, the storage device of Blumenau decrypts the encrypted random number instead of the data that is encrypted using a bus key derived from the nonce. In the disclosure of Blumenau, the encrypted data is the random number, which is used for authenticating a request at the beginning of a data transfer session. The disclosed random number is not used to derive a bus key which in turn is used to encrypt another different data stream, as in the claimed device.

Moreover, Applicants submit that there is no motivation to combine Blumenau with the other cited references. Blumenau is concerned about authenticating access to a storage device. Once the identity of the requestor is verified, subsequent data transfer may or may not be encrypted. On the other hand, in the disclosure of Lotspiech and Utsumi, the entire data transfer is encrypted because the data may be subject to attack along the data transfer path. Absent Applicants' claim that a data bus is connected to a host device in which the encrypted data is to be decrypted, one would not have been motivated to combine Blumenau with the other references as these references have divergent objectives. Accordingly, the proposed combination is inapposite.

Analogous discussion applies to amended Claims 11 and 18. Accordingly, reconsideration and withdrawal of the obviousness rejection of Claims 1, 11, and 18 are requested.

In regard to Claims 2-9, 12-14, 16, 19-21, 23-24, and 26, these claims depend from independent Claims 1, 11, and 18 and incorporate the limitations thereof. Thus, at least for the reasons mentioned in regard to Claims 1, 11, and 18, these claims are not obvious over Lotspiech in view of Utsumi and Blumenau. Accordingly, reconsideration and withdrawal of the obviousness rejection of Claims 2-9, 12-14, 16, 19-21, 23-24, and 26 are requested.

B. Claims 10, 17, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and Blumenau as applied to claims 2, 14, and 19 above, and further in view of U.S. Patent No. 6,751,321 issued to Kato et al. ("Kato"). Applicants respectfully traverse this rejection.

Applicants submit that Claims 10, 17, and 22 are cancelled.

Moreover, Kato does not cure the defects of the above-cited references for failing to teach or suggest a host device that generates a nonce and decrypts the data that is encrypted based on the nonce. From the cited passage at col. 5, lines 30-50 in Kato, a skilled person would understand that each of the encryptor and the decryptor is locally coupled to a random number generator. The encryptor does not receive a random number from the decryption subsystem via the data bus 105, but rather uses a random number locally generated in the transmit device (Fig.

1). Thus, the cited references do not teach or suggest each of the elements of Claims 1, 11, and 18.

C. Claims 10, 17, and 22 are also rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and Blumenau as applied to claims 2, 14, and 19 above, and further in view of the 1998 ACM article "A Practical Secure Physical Bit Generator" authored by Jakobsson et al. ("Jakobsson").

Applicants submit that Claims 10, 17, and 22 are cancelled.

Moreover, Jakobsson also does not cure the defects of Lotspiech, Utsumi, and Blumenau. Nothing in Jakobsson teaches or suggests a host device that generates a nonce and decrypts the data that is encrypted based on the nonce. Jakobsson merely discloses using certain statistics of a computer hard drive (e.g., the access time) to derive randomness (Introduction). The Examiner has not identified and Applicants have been unable to discern any portion of Jakobsson that mentions data decryption. Thus, there is no motivation to combine Jakobsson with the other references because the concept of data protection is totally lacking in Jakobsson. Thus, the cited references do not teach or suggest each of the elements of Claims 1, 11, and 18.

D. Claims 15 and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and Blumenau as applied to claim 19 above, and further in view of U.S. Pre-Grant Publication No. 2002/0015494 applied for by Nagai, et al. ("Nagai"). Applicants respectfully traverse this rejection.

Claims 15 and 25 depend from independent Claims 11 and 18 and incorporate the limitations thereof. Thus, at least for the reasons mentioned above in regard to Claims 11 and 18, the cited references do not teach or suggest each of the elements of these claims. Nagai does not cure the defects. The Examiner relies on Nagai for teaching the descrambling. However, nothing in Nagai teaches or suggests a host device that generates a nonce and decrypts the data that is encrypted based on the nonce, as recited in Claims 11 and 18. Thus, Lotspiech in view of Utsumi and Blumenau and further in view of Nagai does not teach or suggest each of the elements of Claims 15 and 25. Accordingly, reconsideration and withdrawal of the obviousness rejection of Claims 15 and 25 are requested.

E. Claim 25 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Lotspiech in view of Utsumi and Blumenau as applied to claim 19 above, and further in view of U.S. Patent No. 6,778,757 issued to Kawamae, et al. ("Kawamae").

Claim 25 depends from independent Claim 18 and incorporates the limitations thereof. Thus, at least for the reasons mentioned above in regard to Claim 18, the cited references do not teach or suggest each of the elements of Claim 25. Kawamae does not cure the defects. The Examiner relies on Kawamae for teaching a recordable DVD medium that can contain scrambled content. However, nothing in Kawamae teaches or suggests a host device that generates a nonce and decrypts the data that is encrypted based on the nonce, as recited in Claim 18. Thus, the cited references do not teach or suggest each of the elements of Claim 25. Accordingly, reconsideration and withdrawal of the obviousness rejection of Claim 25 are requested.

CONCLUSION

In view of the foregoing, it is believed that all claims now are now in condition for allowance and such action is earnestly solicited at the earliest possible date. If there are any additional fees due in connection with the filing of this response, please charge those fees to our Deposit Account No. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 3/1, 2006

Thomas Coester
Thomas M. Coester, Reg. No. 39,367

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF TRANSMISSION:
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Amber D. Saunders 3/1/06
Amber D. Saunders Date